Internet Network Monitoring Using Snort Integrated with Email (Case Study of Student Boarding School KH Mas Mansur)

To complete the requirement to achieve S-1 graduate in Informatic Department

Communication and Informatic Faculty

Prepared by:

ALUN PRATAMA

L 200 134 007

INFORMATIC DEPARTMENT

COMMUNICATION AND INFORMATIC FAKULTY

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2017

APPROVAL PAGE

INTERNET NETWORK MONITORING USING SNORT INTEGRATED WITH EMAIL (CASE STUDY OF STUDENT BOARDING SCHOOL KH MAS MANSUR)

SCIENTIFIC PUBLICATION

Prepared by:

ALUN PRATAMA
L 200 134 007

Has been examined and approved for tested by

Supervisor

Ir.Bana Handaga, MT., Ph.D
NIK.793

ENDORSEMENT PAGE

INTERNET NETWORK MONITORING USING SNORT INTEGRATED WITH EMAIL (CASE STUDY OF STUDENT BOARDING SCHOOL KH MAS MANSUR)

BY

ALUN PRATAMA

L 200 134 007

Has been well sustained in front of examiners
Faculty of Communication and Informatics
Universitas Muhammadiyah Surakarta
Day 21, October 2017
And has been proven to be qualified

Examiner:

1. **Ir.Bana Handaga, MT., Ph.D.** (.....)
   (The Chief of Examiner)
2. **Dr. Heru Supriyono, M.Sc.** (.....)
   (Member I of Examiner)
3. **Nurgiyatna, ST., M.Sc., Ph.D.** (.....)
   (Member II of Examiner)

This scientific publication has been accepted as one of the requireements
To obtain a bachelor's degree
Date .....
Knowing,

Dean of	**Head of Study Program**
Faculty of Communication and Informatics	**Informatics**
Nurgiyatna, ST., M.Sc., Ph.D	**Dr. Heru Supriyono, M.Sc.**
NIK : 881	**NIK:970**

STATEMENT

I hereby declare that in this scientific publication there is no work ever submitted for a degree at a college and as far as the author's knowledge there is no work or opinion ever written or published by any other person, except in writing referred to in the manuscript and mentioned in the references. One time if there is a false proved in the statement above, I would take full responsibility on it.

Surakarta, 30 October 2017

Writer

ALUN PRATAMA

L 200 134 007

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA
Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: http://informatika.ums.ac.id. Email: informatika@ums.ac.id

SURAT KETERANGAN LULUS PLAGIASI

360/A.4-II.3/INF-FKI/X/2017

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Informatika menerangkan bahwa :

Nama	:	Alun Pratama
NIM	:	L200134007
Judul	:	Internet Network Monitoring Using Snort Integrated with Email (Case Study of Student Boarding School KH Mas Mansur)
Program Studi	:	Informatika
Status	:	**Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 24 Oktober 2017

Biro Skripsi Informatika

Ihsan Cahyo Utomo, S.Kom., M.Kom.

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA
Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: http://informatika.ums.ac.id. Email: informatika@ums.ac.id


turnitin | Internet Network Monitoring Using Snort Integrated with Email (Case Study of Student Boarding School KH Mas Mansur) | 1 of 20

INTERNET NETWORK MONITORING USING INTEGRATED SNORT WITH EMAIL (CASE STUDY OF STUDENT BOARDING SCHOOL KH MAS MANSUR)

Abstrak

Kebutuhan akan permintaan angka internet saat ini perlu diimbangi dengan peningkatan keamanan pada jaringan computer , keadaan ini menuntut seorang administrator selalu memonitoring jaringan yang berjalan dan memiliki respon yang cepat dalam menangani gangguan atau serangan yang akan terjadi.pesntren Mahasiswa K.H Mas Mansur memiliki sistem local yang berfungsi memudahkan manajemen mahasantri diantaranya 1).Sistem pembayaran Mahasantri bulanan dan hunian 2). Sisstem Absensi makan Mahasantri 3). Sistem penerimaan Mahasantri baru dan ujian Mahasantri baru. Pesantren Mahasiswa K.H Mas Mansur memiliki 372 Mahasantri Aktif dan bertambah setiap tahunnya, jaringan yang ada di pesantren mahasiswa K.H Mas Mansur sudah mulai termanajemen dengan baik, namun ada beberapa hal yang perlu ditambahkan untuk pengembangan keamanan jaringan yang ada yaitu monitoring keamanan jaringan secara realtime terhadap gangguan atau serangan. Melihat dari permasalahan diatas dapat dipahami bahwa jaringan yang saat ini berjalan rentan akan serangan selain hal itu apabila ada serangan pada jaringan administrator belum mengetahui apa yang sebenarnya sedang terjadi sehingga membutuhkan waktu untuk mengatasinya. Penelitian ini bertujuan memonitoring keamanan jaringan internet secara realtime menggunakan Snort dan memberikan notifikasi apabila ada gangguan atau serangan pada jaringan sesuai dengan rule rule yang telah ada dalam snort.pegujian system akan melakukan serangan terhadap jaringan yang ada berupa ICMP test dari computer lain

Kata Kunci: Email, IDS, Keamanan Jaringan, Monitoring, Python, Snort

Page: 5 of 18 Word Count: 5910

Match Overview
6%
1 Submitted to University... 1%
2 wrcose.org 1%
3 www.ubuntuhowtodoit... 1%
4 Submitted to Tarleton ... <1%
5 Submitted to Napier Un... <1%
6 www.ijcaonline.org <1%
7 www.i-scholar.in <1%

INTERNET NETWORK MONITORING USING INTEGRATED SNORT WITH EMAIL (CASE STUDY OF STUDENT BOARDING SCHOOL KH MAS MANSUR)

Abstrak

Kebutuhan akan permintaan angka internet saat ini perlu diimbangi dengan peningkatan keamanan pada jaringan computer , keadaan ini menuntut seorang administrator selalu memonitoring jaringan yang berjalan dan memiliki respon yang cepat dalam menangani gangguan atau serangan yang akan terjadi.pesntren Mahasiwa K.H Mas Mansur memiliki sistem local yang berfungsi memudahkan manajemen mahasantri diantaranya 1).Sistem pembayaran Mahasantri bulanan dan hunian 2). Sisstem Absensi makan Mahasantri 3). Sistem penerimaan Mahasantri baru dan ujian Mahasantri baru. Pesantren Mahasiswa K.H Mas Mansur memiliki 372 Mahasantri Aktif dan bertambah setiap tahunnya, Jaringan yang ada di pesantren mahasiswa K.H Mas Mansur sudah mulai termanajemen dengan baik, namun ada beberapa hal yang perlu ditambahkan untuk pengembangan keamanan jaringan yang ada yaitu monitoring keamanan jaringan secara realtime terhadap gangguan atau serangan. Melihat dari permasalahan diatas dapat dipahami bahwa jaringan yang saat ini berjalan rentan akan serangan selain hal itu apabila ada serangan pada jaringan administrator belum mengetahui apa yang sebenarnya sedang terjadi sehingga membutuhkan waktu untuk mengatasinya. Penelitian ini bertujuan memonitoring keamanan jaringan internet secara realtime menggunakan Snort dan memberikan notifikasi apabila ada gangguan atau serangan pada jaringan sesuai dengan rule rule yang telah ada dalam snort.pegujian system akan melakukan serangan terhadap jaringan yang ada berupa ICMP test dari computer lain

Kata Kunci: Email, IDS, Keamanan Jaringan, Monitoring, Python, Snort

Abstract

The need for demand of Internet number ought to be balanced with increased security on computer networks. This situation requires an administrator to always monitor the running network and response quickly in dealing with the interferences or attacks that may occur. Students Boarding School KH Mas Mansur has a local system which functions are to make student management easier, such as 1) Students' monthly and occupancy payment system; 2). Students meal attendance system; 3) New student's registration system and the test for new students. Students Boarding School KH Mas Mansur has 372 active students and it raises each year. The network in students boarding school KH Mas Mansur has been finely manageable, but there are several things that is necessitated to be added to the development of the network security, that is security network monitoring in real-time against interference or attack. From the problems above it can be concluded that the current running network is vulnerable to attacks, and when there is an attack on the network, administrator does not know what is surely occurred, so it takes time to overcome them. This study aims to monitor the internet network security in real-time using Snort and provide notification if there is an interference or attack on the network in accordance with the rules that are already existed in the Snort. The test of the system will carry out the attacks on existing networks such as ICMP test from another computer

Keywords: Email, IDS, Network Security, Monitoring, Python, Snort

1. INTRODUCTION

Computer network security is a process in preventing and monitoring network usage. It aims to anticipate threats that could disrupt the activities of internet use, one of the application that can be used in network monitoring is Snort. Snort is an NIDS (Network Instrution Detection System) application with light-scale usage (Lanke & Jacob, 2014). Snort uses rules that has been provided or can be made as needed to carry out the detection and recording (logging) to computer network attacks. Snort also has some mode advantages such as sniffer mode, inline mode, packet mode, and logger mode.

Students Boarding School KH Mas Mansur is one of the central unit of Muhammadiyah training. This building was inaugurated on 13 September 2008 by the Rector of Muhammadiyah University of Surakarta. The amount of student currently living in there is around 372 students who are spread throughout the faculties and departments in the university and it increase each year. This Boarding School has graduated 582 students. During in boarding school there are 5 permanent staff from the university, 10 supporting staff and some non-permanent staff as cleaning service and canteen's staff. Student boarding school KH Mas Mansur is led by a director and assisted by a vice director also under the guidance of supervisor council consist of 5 people.

To ease the administrative management, Students boarding school KH Mas Mansur has an information system that runs locally within the system as follow 1) Students' monthly and occupancy payment system; 2) Students meal attendance system; 3) New student's registration system and the test for new students. Beside the system above, a system is being developed to recapitulate the prayers and night class.

There is some things to be added to the network development, which is network monitoring in real-time against interference or attacks. From the problems above we can conclude that the current running network is vulnerable to attacks from people who are not responsible. Based on the trouble, it is necessary to develop a system that can report the activity of the Internet network in real time which then would be sent to the administrator via email so that administrators can quickly take action on problems reported that can be done through the remote server to server by restarting or shutting down the server directly to take reasonable precautions against the possibility that may threat the network.

System creation is divided into four components, between each component connects to each other in carrying out its functions so that the message can be delivered to the administrator. *First,* traffic component watcher. *Second* is snort traffic components watcher. *Third,* network data collection component of Snort logs. *Fourth,* the message sender component from the server to the administrator (e-mail). In this case, Snort is run on the Linux Ubuntu server operating system 16.04.

2. METHODS

In research methodology will explain the stages of designing the network security monitoring system integrated with email designed. Some software that must be prepared are Snort, Barnyard2, Python3 and hardware devices such as computer server and Mikrotik router RB750.

2.1 Computer nerwork desain

Architectural design is executed in order that Snort server computer can connect to the internet and perform monitoring of computer networks from intruders which will enter. Before performing the design, observation of the existing conditions is needed in the field so that some data obtained are in

form of blueprints of computer network that can access internet from the observations, while the blueprints are as follows :

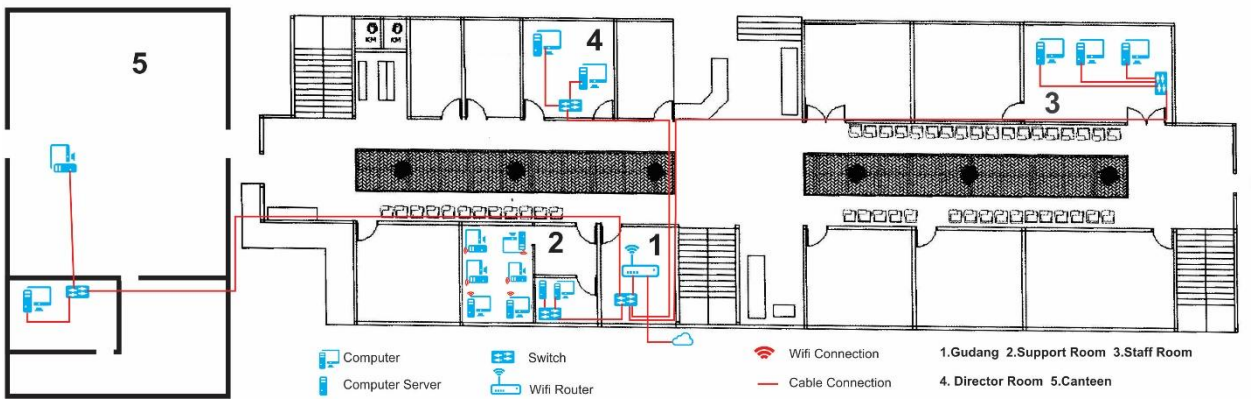

Figure 1 Internet Maps of Pesma Building

From the sketch above can be explained internet from university into a storeroom (1) which then from the room storeroom internet spread spatial the other using cable like to Director room (4), Canteen manager room (5), Employee room (3) and Room server (6) which in every room there is a switch. while for connection to Supporting Staff room (2) using wireless on the router located in storeroom. The image of the existing network in the Student Barding school KH.Mas Mansur in the form of Topology is as follows:

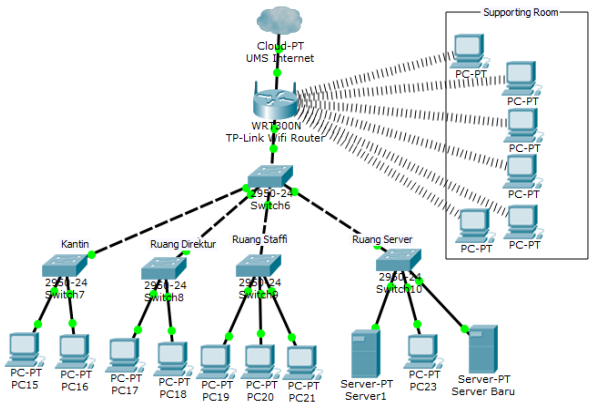

Figure 2 Old Topology Figure

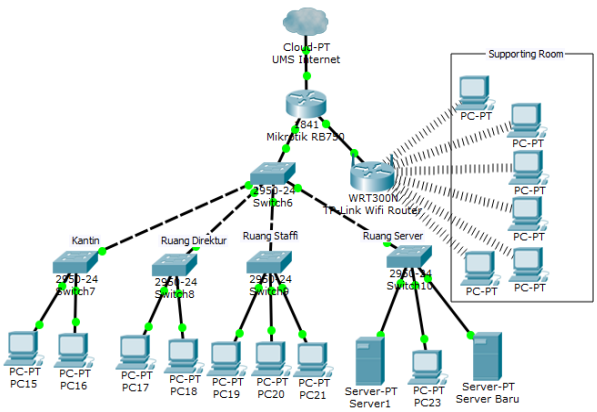

Figure 3 New Design Topology

To be able to implement the security system and network monitoring that will be made then made the network design according to Picture 3 in the existing network added router Mikrotik RB750 duty to connect between the wireless fiber (wi-fi) network and cable as well as the addition of server computer snort which is located in the staff room in one existing network and in a connection with the existing computer system. In its operation snort, has several modes (Rani & Singh, 2011). The first is **Sniffer Mode.** This mode snort serves to capture and view packets passing on the network. The second is **Logger Mode.** This snort mode serves to record all data packets all packets data passing on the network to be analyzed in the future.

Snort also can operate in **Instruction Detection Mode.** This mode serves to detect the snort attack made on computer network which requires this mode to setup multiple files or rules that would differentiate between attack package with normal package, and **Inline Mode** which in this mode snort compares the data packets with iptables rule with libcap and then determine iptables to

drop or allow packets based on Snort rule that has been made. To operate the snort on the network that has been designed, the mode used is the mode of instruction detection mode.

In addition to several operation modes owned by the snort, snort also has the concept of placement. In the implementation of the existing network in boarding school KH Mas Mansur, it uses the concept of a Snort Network Detection System. It can be seen from its name, in this concept, snort monitors data packets not only on the network device engine but also on the entire network according to existing sensors (Sharma & Dixit, 2016). The advantages of this system are the network monitoring coverage is extensive enough and spacious enough to the security while the weakness of this concept is the sensor performs analysis of large amounts of package that requires greater resources.

2.2 System Safety

In this stage, the installation and configuration of components. That component is the network monitoring security system by Snort email integration may work as desired. Some of these components is the analysis of network users, to install and configure snort, installation and Barnyard2 configuration also manufacture programs based on snort that will provide notification to the administrator's email when there is an attack. The detailed explanation will be described in these following points.

2.3 Intallation and Configuration RB750

Mikrotik installation in the network is adjusted with the topology in Picture 3 above. Mikrotik this series has 5 Ethernet port that can be used to connect between one network with the other network. Ethernet 1 is used for internet connections from universities, this Ethernet configuration uses DHCP, to enable DHCP it is necessary to configure DHCP Client provided by mikrotik. Ethernet 2 is used for local network connections using cables, in this Ethernet enable DHCP server function the purpose is to ease in giving IP computer Client, and IP ROUTE configuration to give Gateway IP and the last configuration is NAT Configuration so that those connected via ethernet 2 can access the internet. The configuration done in ethernet 3 is to convert this Ethernet into a switch so that the configuration on Ethernet 3 is the same as in Ethernet 2. The difference is this Ethernet 3 connects wi-fi network to be able to access internet. Wi-fi used in KH.Mas Mansur student Boarding School is TP-Link series

After configuration on each Ethernet used, then configure tools that will be used to obtain data network users in KH.Mas Mansur student Boarding School. Some tools that are used are (1) Graphing tool divided into 2 parts, collecting data internet connection and showing traffic in the form of websites, (2) Torch tools, a tool that has been provided by Mikrotik to monitor traffic on the network in real time. Torch can monitor a particular node so it is helpful to admin in understanding the traffic that occurs on a node based on protocol type, origin, destination address, and type of port. Analysis of the use of computer network aims to see the normal traffic of existing networks in boarding students KH Mas Mansur facilitate the administrator in identifying problems in the network especially there is something unfamiliar occurred in internet traffic. This analysis is expected that administrators can improve the performance of existing networks at this time. This traffic analysis is conducted for one week starting October 10, 2017 and will be finished on October 17, 2017.

2.4 Ubuntu 16.04 Installation

In the security system that will be created, operating system used for the server snort is Linux Ubuntu 16.04 (Tabassum & Mathew, 2014). The installation process of the OS is not described

because there is a documentation from Ubuntu for installation from beginning to end. The choice of OS is because Ubuntu server is open source so that it is free to use without having to pay. Moreover, Ubuntu server does not require large hardware capacity to operate and Ubuntu server version has been stable to use since this version is one of the latest version of Ubuntu server and the kernel uses series 4.4 which is released in January 2016

2.5 Installation and Configuration Snort

Snort is a software-based IDS that is opensource so it is free to be used and modified as needed (Ammad & Hasan, 2016). Snort installation can be performed by downloading the program directly through the official website (www.snort.org). Beside through installation, Snort can be performed with the apt package or synaptic. In this research snort version used is snort 2.9.9.0. Before installation, snort will make sure it has installed daq which in this research is the 2.0.6 version. Function of daq is replacing direct call to libpcap function, daq facilitate operation of various hardware and software without changing snort. After the downloading the file, snort installation is complete. Once installation is complete, snort needs some configuration so that Snort can serve as desired, first thing to do is to setup a folder in accordance with this like the table below:

Table 1 Folder Configuration

Description	Path
Snort data log directory	/ var / log / snort
Snort rule directories	/ etc / snort / rules
	/ etc / snort / so_rules
	/ etc / snort / preproc_rule
	/ usr / local / lib / snort_dynamicrules
IP Snort list directories	/ etc / snort / rules / iplists
Snort dynamic preprocessors	/ usr / local / lib / snort_dynamicpreprocessor

Folders above was made first because after the installation, these folders are available after the folders creation, the next step is to give permissions on each folder permissions is 5775. After the folder, next is snort.conf fileconfiguration. Several functions to change is as follow:

Table 2 Change Configuration in Snort.conf

Line File	Before Change	After Change
Line 45	Ipvar HOME_NET any	Ipvar HOME_NET 192.168.0.0/24
Line 104	Var RULE_PATH ../rules var SO_RULE_PATH ../so_rules var PREPROC_RULE_PATH ../preproc_rules var WHITE_LIST_PATH ../rules var BLACK_LIST_PATH ../rules	var RULE_PATH /etc/snort/rules var SO_RULE_PATH /etc/snort/so_rules var PREPROC_RULE_PATH /etc/snort/preproc_rules var WHITE_LIST_PATH /etc/snort/rules/iplists var BLACK_LIST_PATH /etc/snort/rules/iplists
Line 545	#Include $RULE_PATH/local.rules	Include $RULE_PATH/local.rules

Changes on Line 45 are changes to determine which ip will be monitored with the above changes then the ip to be monitored is ip included in 192.168.0.0/24, the change on line 104 is adjusting the Path to the location of the folder that was created in the previous step while the change on line 545 is to enable local rule and test snort configuration.

2.6 Install Barnyard2

Barnyard2 is an application that serves to connect snort and database. The database used is MySQL thus with help of Barnyard, snort can do output and write on barnyard database has 3 modes. The first mode is batch mode (or one shot). In this mode, barnyard will process specific file then exit. The second mode is a mode of continual. In this mode, barnyard start with specific reading files and continue processing new data. When the data was entered three continual with bookmarks will also use a checkpoint file (or waldo file in the snort world) to track where it is. In the event the barnyard2 process ends while a waldo file is in use, barnyard2 wil l resume processing at the last entry as listed in the waldo file.

For the installation of barnyard2, firstly clone software on github website for clone is github.com/firnsy/barnyard2.git. After the data is downloaded next is the data installation. After the installation is completed the next stage is creating MySQL database for snort that has been installed. After the database is created, later to set up the config file barnyard2.conf done to adjust database that has been made before. After completion of all process above the next step is performing test to check whether between snort and barnyard have been synchronized with look at PHPMyAdmin. If it is already synchronized then database with name of snort will be present

2.7 Python Sending email program

Network administrators may not always be in front of the computer to observe the condition of the existing network especially when there is a vacation time given by the agency to handle. When the administrator is not in front of the computer and the existing network is being infiltrated an intruder then the administrator needs to know it and can take anticipatory action with remote from remote server. In order for administrators to get notifications from snort when there is an intruder in the network in this study the researchers create a python-based program. With this program, Python will read the existing snort database and when an attack on the server python will send an email to the administrator. Before starting the program must first create a .txt file that contains this file numbers will be a benchmark when no new data is entered into a database. The system works as below:

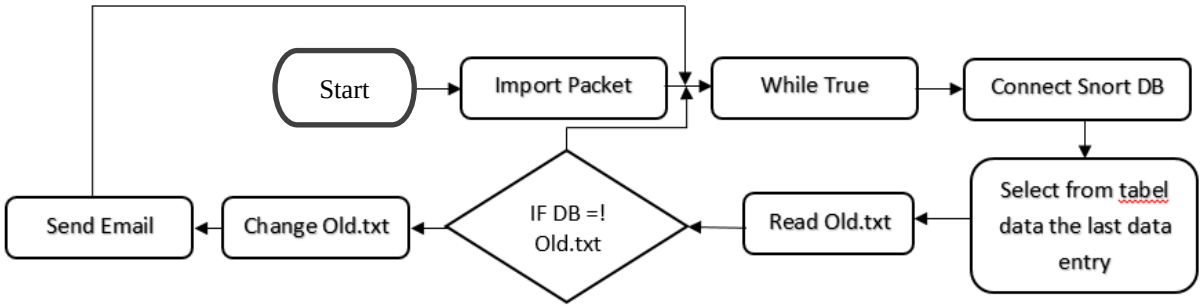

Figure 4 Programming system works

import some packets from the first python mysql.connector. This package serves to connect the program with the destination database. Both this smtplib package serves to activate the smtp in the program. While true, which is used to run this program continuously so that the python is not going to stop (forever loop). Connecting python with snort by entering user, password, host and destination database. After connect it subsequently chose to create a data variable that will be made in comparison to the actual data is the data in table column cid, we only take on the final figures are in column cid and close connection. Initialize new variable, Open file txt and read the contents of the file If the last digit of column cid in the data table is not the same as a txt file, write data in a txt file and change according to the last digit database and then Send an attack notification email.

3. RESULT AND DISCUSSION

In the results and this discussion will show data from internet users as well as tests conducted on snort and send email system using python

3.1 Internet User Data

Internet user data to be displayed is the traffic of internet users wired and wireless fiber, and bandwidth required by pc information systems and application protocol in the network

Table 3. Cable Internet User Traffic

Date	IN		OUT	
	Max	Average	Max	Average
10/10/2017	1.64Mb	55.95Kb	72.08Mb	2.25Mb
11/10/2017	1.63Mb	58.22Kb	70.67Mb	2.37Mb
12/10/2017	1.57Mb	56.37Kb	67.23Mb	2.11Mb
13/10/2017	1.59Mb	32.33Kb	69.63Mb	1.24Mb
14/10/2017	3.11Mb	62.66Kb	55.57Mb	2.06Mb
15/10/2017	1.40Mb	62.75Kb	29.8Mb	1.13Mb
16/10/2017	1.49Mb	65.38Kb	56.57Mb	2.41Mb

Table 3 is table in which contains information about monitoring internet traffic that uses computer wired to the internet connection, The above data was obtained by activating the graphing tools Mikrotik tools RB750 in this research tools monitoring Ethernet 2 on mikrotik. The data shows is the results of monitoring daily. Graphing data show new data every 5 minutes and data will be missing after 24 hours. IN in the table is the data entered into the cable network, the highest data for 24 hours is called IN Max while the average IN is the average traffic entered for 24 hours, OUT is the data out of the cable network while the mean Max and Average equals IN in the table

Table 4. Internet W-Fi User Traffic

Date	IN		OUT	
	Max	Average	Max	Average
10/10/2017	3.59Mb	92.45Kb	7.00Mb	447.12Kb
11/10/2017	3.43Mb	96.13Kb	6.36Mb	527.96Kb
12/10/2017	3.17Mb	82.07Kb	6.72Mb	419.73Kb
13/10/2017	2.16Mb	36.95Kb	11.73Mb	396.52Kb
14/10/2017	2.75Mb	51,48Kb	3.95Mb	321.79Kb
15/10/2017	3.22Mb	66.65Kb	4.16Mb	368.95Kb
16/10/2017	3.44Mb	132.56Kb	9.77Mb	534.42Kb

Table 4 showing monitoring data internet traffic in boarding kh.mas mansur students who use wifi link, the data shows not only computer connected in office but all device connected by wifi as smartphone and laptop. To get data the same by getting traffic the internet using cable distinguish is that monitor ethernet, to get traffic wifi that are monitored is ethernet 3 on mikrotik . The purpose of monitoring traffic on wifi cable and connection is to monitor the condition of the network is actively when things are just not normal in results of monitoring easy to take the next step

Table 5. Information System Bandwidth Server

Date	Download	Upload	Total

10/10/2017	78.0MB	50.3MB	128MB
11/10/2017	78.6MB	25.1MB	104MB
12/10/2017	75.6MB	29.1MB	105MB
13/10/2017	74.5MB	27.7MB	102MB
14/10/2017	102MB	18.8MB	121MB
15/10/2017	23.2MB	1.67MB	24.9MB
16/10/2017	68.6MB	19.9MB	88.5MB

The data shown in table 5 is bandwidth required by the local information system to be able to operate everyday the purpose of collecting data above is to know the normal condition of the bandwidth information system server so when there is something that is not normal administrator can analyze things that happen and perform a response to that. The above data obtained by installing the NetworkX software on the server with the help of this application making it easier to get the data above

3.2 Discussion Intenet user data

The result of observation that has been conducted since the date of 10 to 16 october 2017 it can be explained that internet traffic both cable does not occur a lot of the difference with the exception of what data occuring on may 15 october a significant difference because on that day that is the day on sunday and the office was holiday as for the average traffic in using cable is 56.24kb while to an average traffic out using a cable is 1.90 mb this result obtained from the average summing a whole which already exist at the table and divided by the number of days observation

The results of observations above shows that traffic using wifi more solid day monday to friday on it because at that time were time lectures and several students who lectures know that the wifi and can access them other than that wifi is not used for computer who was in the office but used by a device individuals like smartphone and a laptop to traffic IN on wifi greater than the average cable 79.75kb but out traffic small than cable 430.93kb.

While for bandwith required by server information systems from the table above that servers need less than 150mb in operating it was because when normal days server only in access to absentee purposes eat mahasantri and data input as well as payment transactions that occurred dikantin besides interests above computer servers sometimes used adminidtrator to browse things which are deemed necessary .As it would then bandwith the lowest is on a sunday because on that day the canteen eat shut and the office holiday

3.3 Snort test method

Installation and configuration has been completed in the previous stage, followed by the snort testing phase whether it can detect intruders or not. In this trial modeling used is a network model client/server. In this model required one or more computer servers to manage the data traffic information in computer network computers other than the computer server will be referred to as the client computer in general the server is passive just waiting for various requests from the client then serve the request while the client is the opposite server is active and send requests to the server as well as receive services from the server. From the above explanation for the experiments conducted in this study are simulated in
the form of attacks from the client computer to the server computer. The send email program sends an email automatically when the snort detects an attack.

3.4 The Snort test uses ping rule

Ping works by sending a data packet called Internet Control Message Protocol (ICMP). This ICMP packet is used to transmit network condition information between client and server. The mechanism works when ping to the destination then on the screen will appear some information such as IP that gives echo reply, time (in ms) required ping to get a reply and the last is Time To Live (TTL). After the stop process will be displayed summary of all data packets that have been submitted in addition to it summary also displays the data pack has been received and the calculation of lost data in the middle of the road but it also displays the minimum response time, maximum and average. The results of ping testing with ping command to computer server from client computer produce result like figure below:

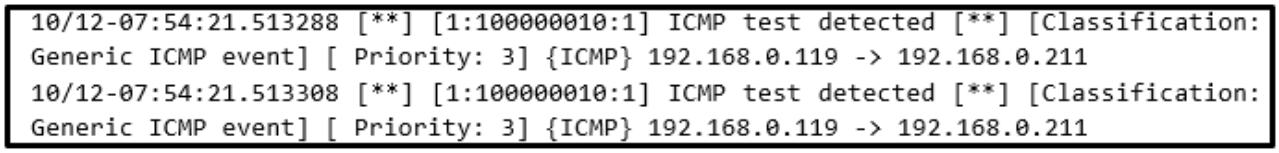

Figure 5 Snort Detect Ping Test

From the picture above, it can be explained that on 12th of 10th at 07:54:21 detected ping attack with ICMP test detected message with sid rule 100000010 detected attack classified with ICMP event and priority of this attack is 3, ping done from IP 192.168. 0.119 to 192.168.0.211. Such attacks can be recognized by the administrator via email in the email. The screenshot of incoming email as follows:

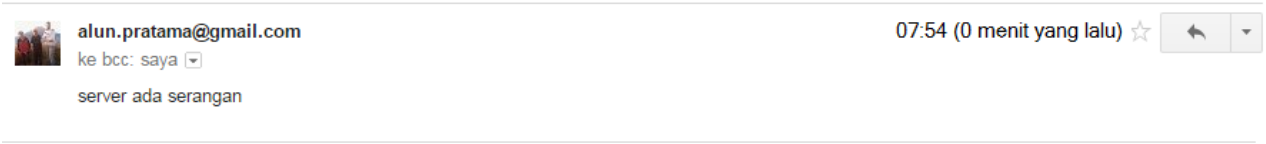

Figure 6 Email Alert PING Test

From the picture above is identified that there is an incoming email from alun.pratama@gmail.com to administrators with email the message server content there is an attack for the incoming message time is 07:54 (0 Minute ago) equal to the time when snort detect snort attacks.

3.5 DDOS Ping Trials

In this ping ddos trial the snort rule will detect the attack when the size bytes sent is more than 100 bytes and the delivery of packets ping more than 7 times the result of the shipment is as follows:

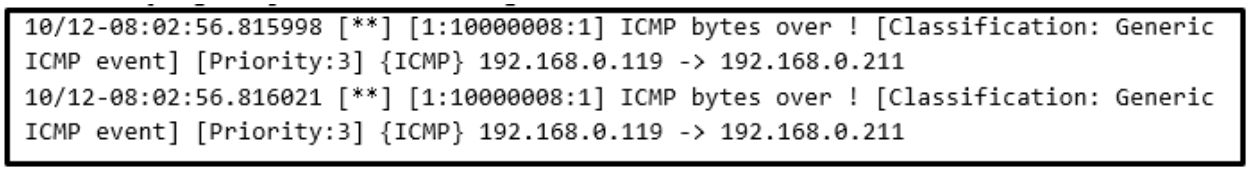

Figure 7 Ping Flood Detected

From the picture above snort detects an attack on the 12th of the 10th month at 08:02 with the message displayed ICMP bytes Over with sid rule 10000008, ping is sent to ip 192.168.0.211 of 192.168.0.119 with priority of attack is 2 and the detected attack is classified in ICMP Event by snort. From the results of the attack detected above there is an incoming email to the administrator to send notification that detects incoming attack messages to the administrator as follows:

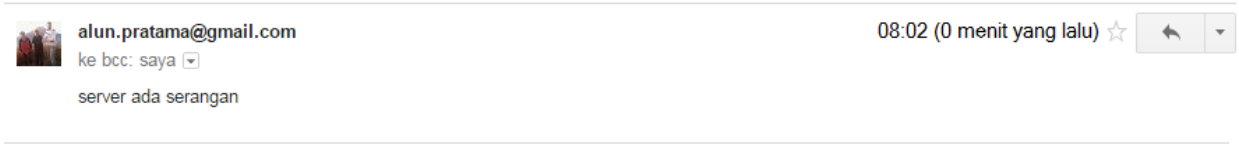

Figure 8 ICMP Flood Email

From Figure 7 displays an incoming message on the administrator email as for the contents of email messages is the server there is sender attack email alun.pratama@gmail.com and the time of incoming messages is 18:02 according to the time on the snort when it detects the attack.

3.6 Testing Port Scan Attack

Port scan test is performed to obtain the open port information on the server computer and to recognize the operating system used and the service is running on the server computer to test this application is used nmap port scan application can be downloaded for free through the internet, from the port scan that snort detects the attack as follows:

```
10/12-08:13:01.732900 [**] [1:9008002:0] NULL Scan [**] [Priority: 0] {TCP}
192.168.0.119:34413 -> 192.168.0.211:22
10/12-08:13:01.859910 [**] [1:9008003:0] XMAS Scan [**] [Priority: 0] {TCP}
192.168.0.119:34413 -> 192.168.0.211:1
```

Figure 9 Port Scan Detected

From Figure 9 it can be seen that the snort detects an attack on the 12th of the 10th month at 8:13 pm with the sid snort rule 90000002 with the NULL Scan message referred to NULL Scan is when scanning all flags changed to off attack originating from 192.168.0.119 addressed to ip 192.168 .02.11 besides the attack snort also detects XMAS Scan seranag with sid rule 90000003 at the same date and time with difference in seconds from IP and addressed to the same IP intent of Xmas Scan is scanning done by sending a FIN, URG, and PUSH to the target PORT, from the above attack the administrator gets the following email:

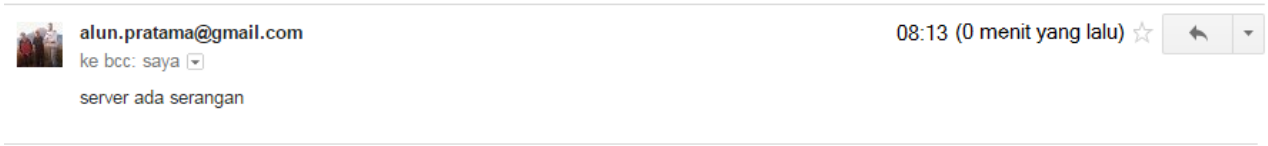

Figure 10 Email Notification Nmap

From Figure 10 displays an incoming message on the administrator's email As for the content of the email message is the server there is an email sender attack alun.pratama@gmail.com and the incoming message time is 08:13 according to the time on the snort when it detects the attack because there are 2 attacks detected then there 2 incoming emails at the same time for notification of detected attacks.

3.7 Test SSH Connection

Testing ssh connection is a test login with putty application on client computer and remote computer remote server port that used for remote this is port 22 from trials conducted snort detect attack as follows:

```
10/12-08:09:30.508426 [**] [1:100001000:0] SSH Connection [**] [Priority:] {TCP}
192.168.0.119:3425 -> 192.168.0.211:22
10/12-08:09:30.705315 [**] [1:100001000:0] SSH Connection [**] [Priority:] {TCP}
192.168.0.119:3425 -> 192.168.0.211:22
```

Figure 11 SSH Connection Detected

Figure 11 shows the detection of login attacks using SSH from another computer attack occurred on the 12th of the 10th month at 08:09 sid snort rule 100001000 with the message displayed SSH Connection detected the attack performed from IP 192.168.0.119 is aimed at IP 192.168.0.211 via port 22, from above attacks the administrator gets an incoming email notification as follows:

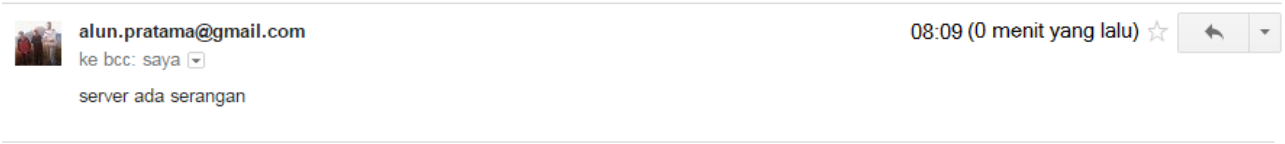

Figure 12 Email SSH Detected

From Figure 12 displays an incoming message on the administrator's email As for the content of the email message is the server there is an email sender attack alun.pratama@gmail.com and the incoming message time is 18:09 according to the time on the snort when it detects the attack.

3.8 Result Of testing

Of several the tests conducted in a snort to sent to administrator notification email, as for the data can be seen in table below :

Tabel 5 Result testing system

No	Testing system scenario	Test Tools	Expected results	Results of testing system	Conclusion
1	Ping Server	Using CMD	Detected	Detected	Successful
2	Ping Flood with Big byte	Using CMD	Detected	Detected	Successful
3	Port Scanning	Using NMAP Application	Detected	Detected	Successful
4	SSH Login	Using Putty	Detected	Detected	Successful

From the testing system in table above, all testing get as expected. System can detect tests carried out by attacker. Detection attack in accordance with rule made starting from ping, ping flood byte, nmap port scan, ssh access. System that built has been tested and can detect any instrusi. The development of technology, so a method of assault progressively hues, the addition of rule in a snort would have a positive impact on security server and tissue protected. With this duty an administrator would be easy in handling server.

Informed about instrusi important for administrator for know the state of current server soluble and network now, so it needs the interaction between servers and the administrator in this research the issue in practice in the form of notification email so administrator not have to be in front of computer is constantly. In addition to the above test results obtained from time against each activity ranging from assault, detection, notification sent until the results of the time entry can be

used to measure the accuracy of speed detection of up to sent alerts. Such data can be seen in the following table:

Tabel 6 Accuray of Speed Detection

No	Types of Attack	Experiment	The Level of Accuracy		
			Early attack	Detected	Send
1	Ping	1	12:43:45	12:43:45	12:43:48
		2	12:45:03	12:45:04	12:45:07
		3	12:47:10	12:47:10	12:47:13
		4	12:48:16	12:48:17	12:48:20
		5	12:49:27	12:49:28	12:49:30
2	Ping Flood Byte	1	12:29:48	12:29:48	12:29:50
		2	12:33:03	12:33:03	12:33:06
		3	12:34:43	12:34:44	12:34:46
		4	12:36:12	12:36:14	12:36:17
		5	12:37:26	12:37:26	12:37:29
3	SSH Connection	1	09:49:20	09:49:22	09:50:06
		2	09:50:50	09:50:51	09:52:01
		3	09:52:30	09:52:31	09:52:50
		4	09:54:18	09:54:19	09:54:58
		5	10:05:55	10:05:56	10:06:30
4	Port Scanning	1	11:05:23	11:05:43	11:05:50
		2	11:08:20	11:08:38	11:08:44
		3	11:10:15	11:10:32	11:10:37
		4	11:11:45	11:12:02	11:12:09
		5	11:13:24	11:13:41	11:13:47

The level of accuracy of time calculated from the difference of time detected and the onset of an attack. From the difference was collected the average speed detection a snort. In addition, speed notification sent also obtained from the difference of time sent to the time detection. Table the difference time will be displayed as follows:

Tabel 7 Difference Time

No	Types of Attack	Experiment	Time (second)	
			The difference between attack and detection	The difference between sent and detected
1	Ping	1	0	3
		2	1	3
		3	0	3
		4	1	3
		5	1	2
2	Ping Flood Byte	1	0	2
		2	0	3
		3	1	2
		4	2	3
		5	0	3
3	SSH Connection	1	2	44
		2	1	60
		3	1	34

		4	1	39
		5	1	34
4	Port Scanning	1	20	7
		2	18	6
		3	17	5
		4	17	7
		5	17	6
Total			101	269
Average			**5.05**	**13.45**

The above data obtained by calculating the time difference in the previous table for the accuracy of time, the time used is the time on the computer server that has been synchronized with the internet time. Table 7 describes for ping attacks, ping flood bytes and SSH takes up to 2 seconds snort detects an attack aimed at the server while for port scanning attacks the average takes 17.8 seconds for attacks can be detected by snort this happens because when the Nmap application run applications need time to process new client requests to do port scanning. In the difference between sent and detected columns the average time required for notifications to be received by the administrator is 13.45 seconds and the time it takes to be able to give attack notification is type SSH attack Connection this happens because the internet connection is present when the attack is detected and the notification is sent and the time it takes for barnyard2 to add data to the snort database.

4. CLOSING

From the writing of the final task with the title of internet network monitoring using snort integrated with email can be concluded first, the design of the network in a building to be a matter of note because with the maximum network design allows administrators to monitor network conditions, second, snort can detect any attacks in KH.Mas Mansur boarding school network with a trial simulation of several attacks with 4 rules of ICMP Test, ICMP bytes Flood, Port Scanning, and SSH Connection, third email-based alert system using python to be one alternative in notification so administrator not continuously in front of computer to observe network conditions. there are some things that can be improved for better results such as administrator update about the rule of attack this is important because the attack varies and ready to attack, other than the notification sent can be modified by notification of the type of attack that is attacking the server.

REFERENCES

Ammad, U., & Hasan, L. (2016). Design and Analysis of Real-time Network Intrusion Detection and Prevention System using Open Source Tools. *International Journal of Computer Applications (0975 – 8887)*, 6-11.

bensooter. (2016, April 10). *Snort 2.9.8.x on Ubuntu 16 LTS with Barnyard2, PulledPork, and Snorby*. Retrieved from github: https://github.com/bensooter/Snort16OnUbuntu

Lanke, N. M., & Jacob, C. R. (2014). Detection of DDOS Attacks Using Snort Detection. *International Journal of Emerging Engineering Research and Technology*, 13-17.

Rani, S., & Singh, V. (2011). SNORT: An Open Source Network Security Tool for Intrusion Detection in Campus Network Environment. *International Journal of Computer Technology and Electronics Engineering*, 1-3.

RaviTeja, G., & M, N. (2017). An Analysis of Various Snort Based Techniques to Detect and Prevent Intrusions in Networks. *In International Conference on Inventive Communication and Computational Technologies* (pp. 10-15). New Delhi: IEEE.

Sharma, S., & Dixit, M. (2016). A Review on Network Intrusion Detection System Using Open. *International Journal of Database Theory and Application*, 61-70.

Tabassum , M., & Mathew, K. (2014). Software Evolution Analysis of Linux (Ubuntu) OS. *International Conference on Computational Science and Technology* (pp. 1-7). Kinabalu: IEEE.

UHTDI. (2016, April 5). *Install configure Snort in Ubuntu 16.04 (Xenial Xerus) with Barnyard2, PulledPork and Snorby*. Retrieved from Ubuntu How to do it: http://www.ubuntu-howtodoit.com/?p=138